Муниципальное бюджетное учреждение
Спортивная школа олимпийского резерва
по легкой атлетике

ПРИКАЗ

«15» июля 2019 г. № 93 г. Прохладный

«О назначении ответственных
за обработку персональных данных
в МБУ «СШОР п легкой атлетике»

В целях исполнения Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» и «Положения по обработке и защите персональных данных

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в МБУ «СШОР по легкой атлетике» заместителя директора Кудрявцеву Татьяну Николаевну.
2. Заместителю директора Кудрявцевой Т.Н. — осуществлять внутренний контроль за соблюдением требований законодательства РФ при обработке персональных данных, в том числе требований к защите персональных данных.
3. Назначить ответственным за сбор, и хранение персональных данных сотрудников учреждения делопроизводителя Сердобинцеву Елену Анатольевну.
4. Назначить ответственным за сбор, и хранение персональных данных воспитанников и их родителей (законных представителей) заместителя директора Кудрявцеву Татьяну Николаевну.
5. Контроль за исполнением настоящего приказа оставляю за собой.

И.О. директора
МБУ «СШОР по легкой атлетике» А.В. Цопанова

С приказом ознакомлена:
Кудрявцева Т.Н.
Сердобинцева Е.А.

Муниципальное бюджетное учреждение
Спортивная школа олимпийского резерва
по легкой атлетике

ПРИКАЗ

«15» июля 2019 г. № 92 г. Прохладный

«О защите персональных данных.»

Руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", в целях защиты персональных данных, обрабатываемых в МБУ «СШОР по легкой атлетике»

ПРИКАЗЫВАЮ:

1 .Утвердить и ввести в действие:
- Положение о порядке обработки персональных данных в МБУ "СШОР по легкой атлетике";
- Перечень сведений ограниченного доступа МБУ «СШОР по легкой атлетике»;
- Перечень должностей, осуществляющих обработку персональных данных в МБУ «СШОР по легкой атлетике» в соответствии с законодательством Российской Федерации;
- Инструкцию по организации учета, использования, передачи и уничтожения электронных носителей персональных данных и другой конфиденциальной информации;
- Модель угроз безопасности персональных данных МБУ «СШОР по легкой атлетике».

2. Ознакомить под подпись всех работников МБУ «СШОР по легкой атлетике» с Положением о порядке обработки персональных данных в МБУ "СШОР по легкой атлетике".
3. Разместить все вышеуказанные документы на официальном сайте учреждения в сети интернет.
4. Контроль за исполнением настоящего приказа оставляю за собой.

И.О. директора
МБУ «СШОР по легкой атлетике»: А.В. Цопанова

Приложение к приказу по МБУ «СШОР
по легкой атлетике» № 92 от 15.07.2019 г.

**Положение о порядке обработки персональных данных
в МБУ "СШОР по легкой атлетике"**

1. Общие положения.

1.1. Настоящее Положение о порядке обработки персональных данных в МБУ "СШОР по легкой атлетике" (далее - Положение) имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение определяет порядок обработки и защиты - персональных данных, в том числе сбора, хранения, передачи и любого другого использования персональных данных работников и субъектов, не являющихся работником МБУ "СШОР по легкой атлетике" (при организации предоставления муниципальных услуг), в соответствии с законодательством Российской Федерации и гарантии конфиденциальности сведений предоставленных субъектом для обработки в МБУ "СШОР по легкой атлетике".

1.3. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативно-правовыми актами, действующими на территории Российской Федерации.

2. Основные понятия

Для целей настоящего Положения используются следующие понятия:

2.1. Оператор персональных данных (далее оператор) - муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели

и содержание обработки персональных данных. В рамках настоящего положения оператором является МБУ «СШОР по легкой атлетике»;

2.2. Персональные данные - любая информация, относящаяся определенному физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

2.3. Субъект - субъект персональных данных.

2.4. Работник (сотрудник) - физическое лицо, состоящее в трудовых отношениях с МБУ «СШОР по легкой атлетике».

2.5. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.6. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно - телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.7. Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

2.8. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.9. Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.10. К персональным данным относятся:

-сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;

- информация, содержащаяся в трудовой книжке работника;

- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;

- сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу;

- сведения об образовании, квалификации или наличии специальных знаний или подготовки;

- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;

- сведения о семейном положении работника;

- информация медицинского характера, в случаях, предусмотренных законодательством;

- сведения о заработной плате работника;
- сведения о социальных льготах;
- сведения о наличии судимостей;
- место работы или учебы членов семьи;
- содержание трудового договора;
- подлинники и копии распоряжений по личному составу;
- основания к распоряжениям по личному составу;
- документы, содержащие информацию по повышению квалификации и переподготовке сотрудника, его аттестация, служебное расследование;
- сведения о награждении государственными наградами Российской Федерации, присвоении почетных, воинских и специальных званий.

3. Обработка персональных данных

3.1. Общие требования при обработке персональных данных.

В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных оператор обязан соблюдать следующие требования:

3.1.1 Ответственным за организацию обработки персональных данных назначается заместитель директора, который выполняет координирующие о контролирующие функции по данному направлению. Ответственными за обработку персональных данных назначаются работники, непосредственно осуществляющие автоматизированную обработку персональных данных в информационных системах, а также работники во исполнение своих должностных обязанностей (инструкций) осуществляющие обработку персональных данных без использования средств автоматизации.

3.1.2. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов РФ, содействия субъектам персональных данных в трудоустройстве, продвижении по службе, обучении, контроля количества и качества выполняемой работы, обеспечения личной безопасности субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

3.1.3. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

3.1.4. При принятии решений, затрагивающих интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.1.5. Работники или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

3.1.6. Субъекты персональных данных, не являющиеся работниками их законные представители имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

3.1.7. Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

3.2. Получение персональных данных.

3.2.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных и дает письменное согласие на их обработку оператором. Форма согласия субъекта на обработку персональных данных представлена в приложении №1 и №2 к настоящему положению (для работников МБУ «СШОР по легкой атлетике» и субъектов персональных данных не являющихся работниками).

3.2.2. В случае недееспособности либо несовершеннолетия субъекта персональных данных все персональные данные субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении персональных данных своего подопечного и дает письменное согласие на их обработку оператором. Форма заявления - согласия на обработку персональных данных подопечного представлена в приложении №3 к настоящему положению.

3.2.3. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

3.2.4. В случае отсутствия согласия на обработку персональных данных оператор разъясняет субъекту обработки персональных данных юридические последствия отказа предоставить свои персональные, данные. Разъяснения юридических последствий дается в письменной форме, типовая Форма разъяснения приведена в приложении №4.

3.2.5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случаях указанных в пункте 3.2.2. настоящего положения согласие может быть отозвано законным представителем субъекта персональных данных. Форма отзыва согласия на обработку персональных данных представлена в приложении №5 к настоящему положению.

3.2.6. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из, которых предоставляется субъекту, второй хранится у оператора. Форма заявления-согласия субъекта на получение его персональных данных от третьей стороны представлена в приложении №6 к настоящему положению.

3.2.7. Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.

3.2.8. Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.9. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3.3 Хранение персональных данных.

3.3.1. Хранение персональных данных субъектов осуществляется на бумажных и электронных носителях с ограниченным доступом.

3.3.2. Личные дела работников хранятся на бумажных носителях в папках, в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа в кабинете директора МБУ «СШОР по легкой атлетике». Личные дела уволенных работников хранятся там же.

3.3.3. Сведения о начислении и выплате заработной платы работников, хранятся в информационных системах бухгалтерского учета и на бумажных носителях в централизованной бухгалтерии.

3.3.4. Заявления и копии документов субъекта, не являющегося работником МБУ «СШОР по легкой атлетике», хранятся в бумажном виде у следующих работников МБУ «СШОР по легкой атлетике»:
- делопроизводитель,
- бухгалтер.

3.3.5. Доступ к персональным данным работников без специального разрешения имеют работники, занимающие в МБУ «СШОР по легкой атлетике» следующие должности:
- директор;
- заместители директора;
- делопроизводитель.

3.3.6. Право доступа к персональным данным субъекта, не являющегося работником МБУ «СШОР по легкой атлетике», имеют:
- руководители и специалисты МБУ «СШОР по легкой атлетике», осуществляющих обработку и хранение персональных данных;
- сам субъект, носитель данных.

3.3.7. Сотрудники МБУ «СШОР по легкой атлетике», хранящие персональные данные на бумажных носителях и имеющие доступ к персональным данным, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования автоматизации», утвержденному постановлением правительства РФ 15 сентября 2008 г. № 687 и обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных, представлена в приложении №8 настоящего Положения.

3.3.8 Лица, замещающие должности, связанные с осуществлением обработки и защиты персональных данных в случае расторжения с ним договора, дают письменное обязательство прекратить обработку персональных данных, ставших известными им с исполнением должностных обязанностей. Типовое обязательство о прекращении обработки персональных данных представлена в приложении № 9 настоящего Положения.

3.4. Передача персональных данных

3.4.1. При передаче персональных данных субъекта оператор обязан соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без Письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами. Форма согласия субъекта на передачу его персональных данных третьей стороне в приложении №7 настоящего положения;

- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;

- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

- передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;

- все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившим запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана. Форма журнала учета передачи персональных данных представлена в приложении № 11 к настоящему положению.

3.4.1. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.4.2. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

3.4.3. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

3.5. Уничтожение персональных данных

3.5.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении (прекращение

деятельности оператора как юридического лица).

3.5.2 Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

3.6. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

3.6.1 Мероприятия по обеспечению безопасности персональных данных при автоматизированной обработке осуществляет ответственный за безопасность персональных данных в МБУ «СШОР по легкой атлетике», согласно его должностной инструкций.

3.6.2 Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных документов уполномоченных федеральных органов исполнительной власти.

3.6.3 Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

3.7. Порядок обработки персональных данных в информационных системах персональных данных без использования средств автоматизации

3.7.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

3.7.2. При неавтоматизированной обработке различных категорий, персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.7.3. При неавтоматизированной обработке персональных данных н, бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

3.7.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав й законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.7.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

3.7.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке:

3.7.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению № 10 к настоящему Положению.

3.7.8. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

3.7.9. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих

распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.7.10. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

3.7.11. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4. Права и обязанности субъектов персональных данных и оператора.

4.1 В целях обеспечения защиты персональных данных субъекты имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
- при отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;
- дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;
- требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

4.2 Для защиты персональных данных субъектов оператор, являющийся муниципальным органом, обязан принять меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", руководствуясь Постановлением Правительства РФ от 21.03.2012 г. №211 и принятыми в соответствии с ним нормативными правовыми актами:

4.2.1. Назначает ответственных за защиту персональных данных в МБУ «СШОР по легкой атлетике», которые будут осуществлять мероприятия (организационные, правовые и технические) по обеспечению безопасности персональных данных при их обработке в информационных системах МБУ «СШОР по легкой атлетике».

4.2.2. Утверждает приказом директора следующие документы:

- о назначении ответственных за организацию обработки персональных данных в МБУ «СШОР по легкой атлетике», ответственных за обработку персональных данных, ответственных за защиту персональных данных;
- положение об обработке персональных данных в МБУ «СШОР по легкой атлетике» или правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами МБУ «СШОР по легкой атлетике»;
- перечень информационных систем персональных данных;
- перечни персональных данных, обрабатываемых в МБУ «СШОР по легкой атлетике» в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг или муниципальных функций;
- перечень должностей работников МБУ «СШОР по легкой атлетике», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- должностные инструкции ответственного за организацию обработки персональных данных и ответственного за защиту персональных данных (за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах);
- типовая форма согласия на обработку персональных данных работников МБУ «СШОР по легкой атлетике», иных субъектов персональных данных (не являющихся работником МБУ «СШОР по легкой атлетике»);
- порядок доступа работников в помещения, в которых ведется обработка персональных данных.

4.2.3. При эксплуатации информационных систем персональных данных МБУ «СШОР по легкой атлетике», являясь оператором таких информационных систем, принимает правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает

установленные уровни защищенности персональных данных;

4.2.4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в МБУ «СШОР по легкой атлетике». Проверки осуществляются ответственным за организацию обработки персональных данных, либо комиссией, состав которой утверждается приказом директора МБУ «СШОР по легкой атлетике». О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает ответственный за организацию обработки персональных данных либо председатель комиссии. Оформляется протокол внутреннего контроля;

4.2.5. Осуществляет ознакомление работников МБУ «СШОР по легкой атлетике» (под расписку), непосредственно осуществляющих обработку персональных данных и защиту персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), настоящим Положением и другими локальными актами учреждения по вопросам обработки персональных данных и (или) организуют обучение указанных служащих; по запросу ознакомить субъекта персональных данных, не являющегося работником, или в случае недееспособности либо несовершеннолетия субъекта, его законных представителей с настоящим положением и его правами в области защиты персональных данных;

4.2.6. Осуществляет передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

4.2.7. По требованию субъекта или его законного представителя предоставляет ему полную информацию о его персональных данных и обработке этих данных.

4.2.8. Уведомляет Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным законом "О персональных данных";

5 Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

5.1 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

5.2 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

6. Заключительные положения

6.1. Настоящее Положение вступает в силу с момента его подписания.

6.2. Настоящее Положение доводится до сведения всех работников МБУ «СШОР по легкой атлетике» под роспись.

Приложение № 1 к Положению о порядке обработки персональных данных в МБУ "СШОР по легкой атлетике" утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г.

Согласие субъекта (работника МБУ «СШОР по легкой атлетике») на обработку персональных данных.

Я,_____ , паспорт серии _____, номер _____ , выданный _____ _ _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие МБУ «СШОР по легкой атлетике», расположенной по адресу: г.о. Прохладный, Комсомольский парк б/н, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно:

- сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;
- информация, содержащаяся в трудовой книжке работника;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу.
- сведения об образовании, квалификации или наличии специальных знаний или подготовки;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- сведения о семейном положении работника;
- информация медицинского характера, в случаях, предусмотренных законодательством;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- сведения о наличии судимостей;
- место работы или учебы членов семьи;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- основания к приказам поличному составу;
- документы, содержащие информацию по повышению квалификации и переподготовке сотрудника, его аттестация, служебное расследование;
- сведения о награждении государственными наградами Российской Федерации, присвоении почетных, воинских и специальных званий.

Все персональные данные могут быть использованы для сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), обработки, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе (а именно: использования вышеуказанных данных для формирования кадровых документов, работы в информационной системе для осуществления расчетов работодателя со мной как работником, обезличивания, блокирования, уничтожения. Обработка персональные данных может осуществляться посредством внесения их в электронную базу данных, включения в списки (реестры), отчетные формы и другое. Оператор имеет право на обмен (прием и передачу) персональных данных с другими организациями с использованием электронных носителей или по каналам связи в случаях, предусмотренных действующим законодательством.

Я утверждаю, что ознакомлен (а) с документами МБУ «СШОР по легкой атлетике», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____»_____20 г.

(подпись)

Приложение № 2 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Согласие субъекта (не являющегося работником МБУ «СШОР по легкой атлетике») на обработку персональных данных.

Я, ____, паспорт серия ______, номер_________, выданный_____________________________________

____

В соответствии с Федерльным законом от 27.07.2006 г. № 152 – ФЗ «О персональных данных» даю согласие МБУ «СШОР по легкой атлетике», расположенному по адресу: КБР, г. Прохладный, [illegible], 2/а на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно:

- сведения, содержащиеся в основном документе, удостоверяющем личность субъекта;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- сведения о семейном положении;
- место работы и учебы членов семьи;
- другие документы:
-____
-____
-____
-____
-____
-____
-____

Для обработки в целях

____

____

____

____

(указать цели обработки)

Я утверждаю, что ознакомлен(а) с документами МБУ «СШОР по легкой атлетике», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«____»______________20 г.

(подпись)

Приложение № 3 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Заявление – согласие субъекта
на обработку персональных данных подопечного.

Я, _____, паспорт серия _____, номер_____, выданный_____
_____

В соответствии с Федерльным законом от 27.07.2006 г. № 152 – ФЗ «О персональных данных» даю согласие МБУ «СШОР по легкой атлетике», расположенному по адресу: КБР, г. Прохладный, Комсомольский парк, б/н на автоматизированную, а также без использования средств автоматизации обработку персональных данных моего (ей) сына (дочери, подопечного)
_____
(Ф.И.О. сына, дочери, подопечного)
а именно:_____
_____
_____
(указать состав персональных данных (Ф.И.О., паспортные данные, адрес……)
Для обработки в целях _____
_____
_____
(указать цели обработки)

Я утверждаю, что ознакомлен(а) с документами МБУ «СШОР по легкой атлетике», устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.
Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока.
Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____» _____ 20 г.

(подпись)

Приложение № 4 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

Мне_____
(Ф.И.О.)

Разъяснены юридические последствия отказа предоставить свои персональные данные оператору МБУ «СШОР по лёгкой атлетике».

В соответствии с Постановлением Правительства РФ от 21.03.2012 г. № 211 «Перечень мер направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных»» пунктом 2.10 Положения об обработке персональных данных в МБУ «СШОР по легкой атлетике» определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с _____
(решением вопросов местного значения, с указанием муниципальной услуги, реализации права на труд, право

_____
избирать и быть избранным в органы местного самоуправления, права на пенсионное обеспечение, медицинское

_____
страхование работников)

Я предупрежден, что в случае несогласия на обработку персональных данных (далее нужное подчеркнуть):

1. Администрацией МБУ «СШОЛР по легкой атлетике» при решении вопросов местного значения мои права могут быть реализованы на в полном объеме.
2. Право на труд, право избирать и быть избранным в органы местного самоуправления, право на пенсионное обеспечение и медицинское страхование работников не может быть реализовано в полном объеме, а трудовой договор подлежит расторжению.

«_____»_____20 г.

(подпись)

Приложение № 5 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Отзыв согласия на обработку персональных данных

МБУ «СШОР по легкой атлетике»

_____

(Ф.И.О. субъекта персональных данных)

_____

(Адрес регистрации субъекта персональных данных)

_____

(Номер основного документа удостоверяющего личность)

_____

(Дата выдачи указанного документа)

_____

(Наименование органа выдавшего документа)

Заявление.

Прошу Вас прекратить обработку моих персональных данных в связи с

_____ .

(указать причину)

«____»_____ 20____ г. _____ _____

(подпись) (расшифровка подписи)

Приложение № 6 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Заявление – согласие субъекта
на получение его персональных данных у третьей стороны.

Я, _____, паспорт серия _____, номер_____, выданный_____
_____
в соответствии со статьей 86 Трудового Кодекса Российской Федерации _____ на получение моих персональных данных, а именно:
(согласен/не согласен)
_____
_____
_____
_____
_____
_____
_____
(указать состав персональных данных (Ф.И.О. , паспортные данные, адрес и .т.д.)

Для обработки в целях:
_____
_____
_____
_____
_____
_____
_____
(указать цели обработки)

У следующих лиц:
_____
_____
_____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

«____»_____ 20____ г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 7 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Заявление – согласие субъекта
на передачу его персональных данных у третьей стороны.

Я, _____, паспорт серия _____, номер_____, выданный_____
_____
в соответствии со статьей 88 Трудового Кодекса Российской Федерации _____ на передачу моих персональных данных, а именно:
(согласен/не согласен)

_____
_____
_____
_____
_____
_____
_____

(указать состав персональных данных (Ф.И.О. , паспортные данные, адрес и .т.д.)

Для обработки в целях:

_____
_____
_____
_____
_____
_____
_____

(указать цели обработки)

Следующим лицам:

_____
_____
_____
_____

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их передачу.

«____»_____ 20____ г. _____ _____
(подпись) (расшифровка подписи)

Приложение № 8 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

Соглашения о неразглашении персональных данных

Я, _____, паспорт серия _____, номер_____, выданный_____ _____

года, понимаю, что получаю доступ к персональным данным работников МБУ «СШОР по легкой атлетике».

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все требования, описанные в Положении о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике».

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи; паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.

«____»_____ 20____ г. _____ _____

(подпись) (расшифровка подписи)

Приложение № 9 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г

ТИПОВОЕ СОГЛАШЕНИЕ
о прекращении обработки персональных данных лица, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним договора

Я, _____

(Ф.И.О.)

_____

(должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной контракта (договора), освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мце в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006 г. № 152- ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

«____»_____ 20____ г. _____ _____

(подпись) (расшифровка подписи)

Приложение № 10 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике»

ЖУРНАЛ
УЧЕТА НОСИТЕЛЕЙ ИНФОРМАЦИИ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Дата начала ведения журнала: _____

Дата окончания ведения журнала: _____

Количество листов: _____

Дата поступления	Рег. №	Откуда поступил	Вид носителя	Кол-во носителей	Номер и дата сопроводи-тельного документа	Учётные номера носителя	Кому передан носитель	Дата передачи носителя	Дата и номер акта уничтожения	Ф.И.О. Передав-шего	Ф.И.О. Получив-шего	Роспись
1	2	3	4	5	6	7	8	9	10	11	12	13

Приложение № 11 к Положению о порядке обработки персональных данных в МБУ «СШОР по легкой атлетике» утвержденном Приказом по МБУ «СШОР по легкой атлетике»

Журнал учета передачи персональных данных

	Сведения о запрашивающем лице	Состав запрашйваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/ отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника

Приложение к приказу по МБУ «СШОР по легкой атлетике» № от

Модель угроз безопасности персональных данных МБУ «СШОР по легкой атлетике».

I. Перечень обозначений и сокращений.

1. АРМ - автоматизированное рабочее место;
2. ИР - информационный ресурс;
3. ИСПДн - информационная система персональных данных;
4. КЗ - контролируемая зона;
5. ПДн - персональные данные;
6. ПО - программное обеспечение;
7. ПТС - программно-технические средства;
8. ПЭМИН - побочные электромагнитные излучения и наводки;
9. СЗИ - средства защиты информации;
10. СКЗИ - средства криптографической защиты информации;
11. ФСБ - Федеральная служба безопасности;
12. ФСО - Федеральная служба охраны;
13. ФСТЭК - Федеральная служба по техническому и экспертному контролю.

II. Общие положения.

1. Настоящая модель угроз безопасности персональных данных (далее - Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке (далее - Учреждение). Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости ИСПДн, характерные для данной ИСПДн, реализуя тем самым угрозы информационной безопасности.
2. В Модели дается обобщенное описание ИСПДн, состав, категории и предполагаемый объем обрабатываемых ПДн с последующей классификацией ИСПДн.
3. Модель описывает потенциального нарушителя безопасности ПДн и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной ИСПДн.
4. Настоящая Модель разработана в соответствии с требованиями Федерального законодательства и федеральных органов по защите персональных данных.

III. Характеристика объекта информатизации

В учреждении существуют следующие типы ИСПДн:

1. ИСПДн ведения бухгалтерского учета, расчета заработной платы.
ИСПДн передачи информации, в том числе ПДн, в целях исполнения Федеральных законов.
2. Состав ИСПДн и обрабатываемых в них персональных данных.
3. В качестве объекта информатизации Школы выступают:

1. Автономные автоматизированные рабочие места (АРМ).
2. Локальные вычислительные сети.

4. В зависимости от характеристик и особенностей отдельных объектов часть

вычислительных средств данных предприятий подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

5. Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта ПДн), так и с электронных носителей информации.

6. ИСПДн предполагают распределенную (на АРМ) обработку и хранение ПДн.

7. Персональные данные субъектов ПДн могут выводиться из ИСПДн с целью передачи персональных данных субъектов Учреждения, как в электронном, так и в бумажном виде.

8. Контролируемой зоной (КЗ) ИСПДн являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, сетевое и телекоммуникационное оборудование ИСПДн. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

IV. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных

1. На основе характеристик и особенностей используемых ИСПДн и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов ПДн, обрабатываются в Учреждении информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в ИСПДн Учреждения не обрабатываются.

2. Для ИСПДн Школы актуальны угрозы 2 типа - угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе. Согласно подпункту «б» пункта 11 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», для ИСПДн Школы требуется обеспечить 3-ий уровень защищенности персональных данных при их обработке в информационной системе.

V. Способы нарушения характеристик безопасности персональных данных

1. Исходя из перечня персональных данных, обрабатываемых в ИСПДн, существуют следующие способы нарушения характеристик безопасности ПДн:
   - хищение персональных данных сотрудниками Учреждения для использования в корыстных целях;
   - передача финансовой, адресной, юридической и прочей информации о субъекте ПДн третьим лицам;
   - несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам Школы;
   - несанкционированное получение персональных данных третьими лицами;
   - уничтожение финансовой, адресной и прочей информации о субъекте ПДн;
   - модификация финансовой, адресной и прочей информации о субъекте ПДн;
   - блокирование финансовой, адресной и прочей информации о субъекте ПДн;
   - ввод некорректной финансовой, адресной и прочей информации о субъекте ПДн;
   - передача некорректной финансовой, адресной и прочей информации о субъекте ПДн;
   - искажение архивной информации по субъекту ПДн;

- уничтожение архивной информации по субъекту ПДн.

VI. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных

1. Под угрозами безопасности персональных данных при их обработке в ИСПДн понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности ПДн при их обработке в ИСПДн могут быть связаны как с непреднамеренными действиями персонала ИСПДн, так и со специально осуществляемыми неправомерными действиями отдельных организаций и граждан, а также иными источниками угроз. Неправомерные действия могут исходить также и от сотрудников Учреждения в случае, когда они рассматриваются в качестве потенциального нарушителя безопасности ПДн.

2. В целях формирования систематизированного перечня угроз безопасности ПДн при их обработке в ИСПДн и разработке на их основе частных (детализированных) моделей применительно к конкретному виду ИСПДн, угрозы безопасности персональным данным в ИСПДн можно классифицировать в соответствии со следующими признаками:
- по видам возможных источников угроз;
- по типу ИСПДн, на которые направлена реализация угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);
- по способам реализации угроз;
- по используемой уязвимости;
- по объекту воздействия.

3. Для ИСПДн существуют следующие классы угроз безопасности ПДн:

По видам возможных источников угроз безопасности персональных данных:
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к ИР ИСПДн, включая пользователей, реализующие угрозы непосредственно в ИСПДн;
- угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
- угрозы, возникновение которых напрямую зависит от свойств техники, используемой в ИСПДн;
- угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена угроза:

По структуре ИСПДн, на которые направлена угроза, необходимо рассматривать следующие классы угроз:
- угрозы безопасности данных, обрабатываемых в ИСПДН на базе автоматизированных рабочих мест;
- угрозы безопасности данных, обрабатываемых в ИСПДН на базе локальных информационных систем.

По способам реализации угроз

По способам реализации угроз выделяют следующие классы угроз:
- угрозы, связанные с несанкционированным доступом к ПДн (в том числе угрозы внедрения вредоносных программ);
- угрозы утечки ПДн по техническим каналам утечки информации (ТКУИ);
- угрозы специальных воздействий на ИСПДн.

По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными)

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
- угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование данных.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системного программного обеспечения (ПО);
- угрозы, реализуемые с использованием уязвимости прикладного ПО; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в ИСПДн аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;
- угрозы безопасности ПДн, передаваемых по сетям связи;
- угрозы прикладным программам, с помощью которых обрабатываются ПДн;
- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

VII. Характеристика источников угроз безопасности персональных данных в ИСПДн

1. В отношении ИСПДн могут существовать три типа источников угроз безопасности ПДн:

1. Антропогенные источники угроз безопасности ПДн.
2. Техногенные источники угроз безопасности ПДн.
3. Стихийные источники угроз безопасности ПДн.

Антропогенные источники угроз безопасности ПДн

В качестве антропогенного источника угроз для ИСПДн необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами ИСПДн, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании ИСПДн и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в ИСПДн. К таким источникам можно отнести персонал поставщиков различного рода

услуг, персонал надзорных организаций и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников - умышленная дезорганизация работы, вывод систем Организации из строя, искажение информации за счет проникновения в ИСПДн путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств ИСПДн. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками Учреждения, имеющих доступ к ИР ИСПДн. К подобным угрозам, в частности, относятся:

- непредумышленное искажение или удаление программных компонентов;
- внедрение и использование неучтенных программ;
- игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИСПДн, включая средства защиты информации. В частности:
- нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
- предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
- настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
- несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

- угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к ИСПДн, включая пользователей ИСПДн и иных сотрудников Учреждения, реализующими угрозы непосредственно в ИСПДн (внутренний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);
- угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к ИСПДн и реализующими угрозы по ТКУИ.

Техногенные источники угроз безопасности ПДн.

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы ИСПДн: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в ИСПДн, а также вредоносное

программное обеспечение и аппаратные закладки.

Аппаратная закладка.

Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы:

- сбора и накопления ПДн, обрабатываемых и хранимых в ИСПДн;
- формирования ТКУИ.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла ИСПДн.

Носитель вредоносной программы

В качестве носителя вредоносной программы в ИСПДн может выступать аппаратный элемент средств вычислительной техники из состава ИСПДн или ПО, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего ПО ИСПДн, в качестве ее носителя выступают:

- внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
- встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства - видеоадаптера, сетевой платы, устройств ввода/вывода и т.д.)
- микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим ПО, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

- пакеты передаваемых по сети ИСПДн сообщений;
- файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Стихийные источники угроз безопасности ПДн.

Стихийные источники угроз отличаются большим разнообразием и непредсказуемостью и являются, как правило, внешними по отношению к Учреждению. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой ИСПДн и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности ПДн.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности ПДн, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации ИСПДн.

VIII. Модель нарушителя безопасности персональных данных

1. Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

- Безопасность ПДн в ИСПДн обеспечивается средствами защиты информации ИСПДн, а также используемыми в них информационными технологиями, техническими и

программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;
- Средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СЗИ требований;
- СЗИ не могут обеспечить защиту ПДн от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту ПДн от раскрытия лицами, которым предоставлено право на доступ к этим данным).

2 .Описание нарушителей.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИСПДн, все физические лица могут быть отнесены к следующим двум категориям:
- категория I - лица, не имеющие права доступа в контролируемую зону ИСПДн;
- категория II - лица, имеющие право доступа в контролируемую зону ИСПДн.

Все потенциальные нарушители подразделяются на:
- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИСПДн;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИСПДн.

В качестве внешнего нарушителя, кроме лиц категории I, должны рассматриваться также лица категории II, находящиеся за пределами КЗ.
В отношении ИСПДн, в качестве внешнего нарушителя из числа лиц категории I, могут выступать:
- бывшие сотрудники Учреждения;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
- представители преступных организаций.

Внешний нарушитель может осуществлять:
- перехват обрабатываемых техническими средствами ИСПДн ПДн за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
- деструктивные воздействия через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
- несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
- перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно- техническими мерами;
- атаки на ИСПДн путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам (ИР) ИСПДн.

К первой группе относятся сотрудники Учреждения, не являющиеся зарегистрированными пользователями и не допущенные к ИР ИСПДн, но имеющие санкционированный доступ в КЗ.

Лицо данной группы может:
- располагать именами и вести выявление паролей зарегистрированных пользователей ИСПДн;
- изменять конфигурацию технических средств обработки ПДн, вносить программно-аппаратные закладки в ПТС ИСПДн и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

Ко второй группе относятся зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ИР ИСПДн с рабочего места. К этой категории относятся сотрудники Учреждения, имеющие право доступа к локальным ИР ИСПДн для выполнения своих должностных обязанностей.

Лицо данной группы:

- обладает всеми возможностями лиц первой категории;
- знает, по меньшей мере, одно легальное имя доступа;
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к ИР ИСПДн;
- располагает ПДн, к которым имеет доступ.

К третьей группе относятся зарегистрированные пользователи подсистем ИСПДн, осуществляющие удаленный доступ к ПДн по локальной сети Учреждения.

Лицо данной группы:

- обладает всеми возможностями лиц второй категории;
- располагает информацией о топологии сети ИСПДн и составе технических средств ИСПДн;
- имеет возможность прямого (физического) доступа к отдельным техническим средствам (ТС) ИСПДн.

К четвертой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности ИСПДн.

Лицо данной группы:

- обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте ИСПДн;
- обладает полной информацией о технических средствах и конфигурации сегмента ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте ИСПДн;
- имеет доступ ко всем техническим средствам сегмента ИСПДн;
- обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента ИСПДн.

К пятой группе относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

- обладает полной информацией о системном, специальном и прикладном ПО, используемом в ИСПДн;
- обладает полной информацией о ТС и конфигурации ИСПДн
- имеет доступ ко всем ТС ИСПДн и данным;
- обладает правами конфигурирования и административной настройки ТС ИСПДн.

К шестой группе относятся зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности Учреждения, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

К седьмой группе относятся лица из числа программистов - разработчиков

сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн.

Лицо данной группы:

- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн.

К восьмой группе относятся персонал, обслуживающий ТС ИСПДн, а также лица, обеспечивающие поставку, сопровождение и ремонт ТС ИСПДн.

Лицо данной группы:

- обладает возможностями внесения закладок в ТС ИСПДн на стадии их разработки, внедрения и сопровождения;
- может располагать фрагментами информации о топологии ИСПДн, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о ТС защиты информации в ИСПДн.

2. Предположения о возможностях нарушителя.

Для получения исходных данных о ИСПДн нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям ИСПДн.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения ИСПДн ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

- предотвращение и пресечение несанкционированных действий;
- подбор и расстановку кадров;
- допуск физических лиц в контролируемую зону и к средства вычислительной техники;
- контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о ИСПДн в объеме, необходимом для решения вопросов создания и преодоления средств защиты ПДн, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к ИР с использованием только штатных программно-технических средств ИСПДн без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем ИСПДн, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения ИСПДн.

3. Предположения об имеющихся у нарушителя средствах атак.

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами КЗ) может использовать следующие средства доступа к защищаемой информации:

- доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;

- специально разработанные технические средства и программное обеспечение;
- средства перехвата и анализа информационных потоков в каналах связи;
- специальные технические средства перехвата информации по ТКУИ;
- штатные средства ИСПДн (только в случае их расположения за пределами КЗ).

Внутренний нарушитель для доступа к защищаемой информации, содержащей ПДн, может использовать только штатные средства ИСПДн. При этом его возможности по использованию штатных средств зависят от реализованных в ИСПДн организационно-технических и режимных мер.

4. Описание каналов атак.

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в ИСПДн, являются:

- каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
- электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
- бумажные носители информации;
- штатные программно-аппаратные средства ИСПДн;
- кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от НСД к информации организационно - - техническими мерами;
- незащищенные каналы связи; ТКУИ.

5. Тип нарушителя при использовании в ИСПДн криптографических средств защиты информации.

При обмене информацией между ИСПДн и внешними по отношению к предприятию информационными системами необходимо использование средств криптографической защиты информации (СКЗИ).

Уровень криптографической защиты персональных данных, обеспечиваемой СКЗИ, определяется путем отнесения нарушителя, действиям которого должно противостоять СКЗИ, к конкретному типу, и базируется на подходах, описанных в «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации».

Тип нарушителя и класс СКЗИ должен определяться в соответствии с таблицей.

Таблица - соответствие типов нарушителя и класса СКЗИ

Группа внутреннего нарушителя	Тип нарушителя	Класс СКЗИ
Группа 1	Н2	КС2
Группа 2	Н3	КС3
Группа 3	Н3	КС3
Группа 4	Н3	КС3
Группа 5	Н3	КС3
Группа 6	Н3	КС3
Группа 7	Н5	КВ2
Группа 8	Н4	КВ1

Внешний нарушитель относится к типу Н1. При этом, если он обладает возможностями по созданию способов и подготовки атак, аналогичными соответствующим возможностям внутреннего нарушителя типа Hi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Hi.

IX. Актуальные угрозы безопасности персональных данных в информационных системах персональных данных

1. Для выявления из всего перечня угроз безопасности ПДн актуальных для ИСПДн оцениваются два показателя:
   - уровень исходной защищенности ИСПДн;
   - частота (вероятность) реализации рассматриваемой угрозы.
2. Уровень исходной защищенности информационной системы персональных данных

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Перечень данных характеристик и показатели защищенности ИСПДн, зависящие от них, показаны в таблице.

3. Показатели, относящиеся к Учреждению выделены жирным курсивом.

Для определения исходной защищенности ИСПДн должно быть рассчитано процентное соотношение каждого уровня защищенности ко всем характеристикам, имеющим место для ИСПДн.

Таблица 9.1 - Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень**		
	Высокий	Средний	Низкий
По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			■
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			■
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации		■	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		■	
Локальная ИСПДн, развернутая в пределах одного здания	■		
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования			■
ИСПДн, имеющая одноточечный выход в сеть общего пользования		■	
ИСПДн, физически отделенная от сети общего пользования	■		
По встроенным (легальным) операциям с записями баз ПДн			
чтение, поиск	■		
запись, удаление, сортировка		■	
модификация, передача			■
По разграничению доступа к персональным данным			

ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			
Интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации -владельцу данной ИСПДн			
По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать личность)			
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без			
ИСПДн, предоставляющая всю базу данных с ПДн			
ИСПДн, предостаоляющтя часть ПДн			
ИСПДн, не предоставляющие никакой информации			
Количество решений	1	2	1
Общее количество решений	4		

4. Принимается, что ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные уровню «средний».

В случае, если не менее 70% характеристик ИСПДн относится к уровню «не ниже среднего», а остальные к уровню «низкий», то исходная защищенность ИСПДн будет среднего уровня.

Во всех остальных случаях ИСПДн будет иметь низкий уровень защищенности. Исходя из критериев оценки, делаем вывод, что ИСПДн Учреждения имеет средний уровень защищенности.

5. Определение актуальных угроз безопасности персональных данных.

Для оценки уровня исходной защищенности вводится коэффициент исходной защищенности Y1, который может принимать значения:

0 - для высокой степени исходной защищенности;

5 - для средней степени исходной защищенности;

10 - для низкой степени исходной защищенности.

Следующим параметром, необходимым для определения актуальности угроз безопасности ПДн, является частота (или вероятность) реализации угрозы, под которой понимается определенный экспертным путем показатель, характеризующий вероятность реализации конкретной угрозы безопасности ПДн для ИСПДн в

реальных условиях ее функционирования. Вводится четыре значения этого показателя, обозначаемого как Y2:
- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Данный показатель принимает следующие значения:
0 - для маловероятной угрозы;
2 - для низкой вероятности угрозы;
5 - для средней вероятности угрозы;
10 - для высокой вероятности угрозы.

Используя значения приведенных выше показателей Y1 и Y2, вычисляется коэффициент реализуемости угрозы Y, определяемый соотношением Y = (Y1+Y2)/20.

В зависимости от своего значения этот коэффициент принимает значения:
0 < Y < 0,3 - реализуемость угрозы признается низкой;
0,3 < Y < 0,6 - реализуемость угрозы признается средней;
0,6 < Y < 0,8 - реализуемость угрозы признается высокой;
Y > 0,8 — реализуемость угрозы признается очень высокой.

Далее дается оценка опасности каждой угрозы ПДн для ИСПДн. Данная оценка носит экспертный характер и получается путем опроса экспертов в области безопасности информации. Данная оценка имеет три значения:
- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов ПДн;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

После просчета всех показателей производится оценка актуальности каждой угрозы безопасности ПДн при их обработке в ИСПДн исходя из матрицы, приведенная в таблице 9.2:

Таблица 9.2 - Матрица расчета актуальности угроз безопасности ПДн

Реализуемость угрозы	Показатель опасности угрозы		
	Низка	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основании положений модели угроз, модели нарушителя, данных об исходной защищенности ИСПДн (Y1), коэффициенте реализуемости угрозы (Y), вероятности ее реализации (Y2), а также экспертной оценки опасности угрозы, определяется актуальность каждой угрозы безопасности ПДн, обрабатываемых в ИСПДн. (Таблица 9.3):

Таблица 9.3 - Актуальность угроз безопасности ПДн

№ п/п	Угроза безопасности ПДн	Вероятность реализа	Коэффициент реализуе	Оценка опасности угрозы	Оценка актуальности угрозы
1.	Разглашение, передача или утрата атрибутов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная
2.	Нарушение правил хранения атрибутов разграничения доступа к ИСПДн	5	0,75	низкая	актуальная
3.	Несообщение о фактах утраты, компрометации атрибутов разграничения доступа к ИСПДн	10	1,0	высокая	актуальная
4.	Внедрение агентов в число персонала системы	0	0,5	высокая	актуальная
5.	Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)	2	0,6	высокая	актуальная
6.	Ввод ошибочных данных	10	1,0	низкая	актуальная
7.	Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств	5	0,75	высокая	актуальная
8.	Игнорирование организационных ограничений (установленных правил) при работе с ПД	10	1	средняя	актуальная
9.	Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов ИСПДн	0	0,5	высокая	актуальная
10.	Закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;	0	0,5	низкая	Не актуальная
11.	Хищение носителей информации, содержащих ПД	2	0,6	высокая	актуальная
12.	То же, внешний нарушитель	2	0,6	высокая	актуальная
13.	Незаконное получение паролей и других реквизитов разграничения доступа к ИСПДн	5	0,75	средняя	актуальная
14.	То же, внешний нарушитель	2	0,6	средняя	актуальная
15.	Несанкционированная модификация программного обеспечения	5	0,75	высокая	актуальная

16.	То же, внешний нарушитель	2	0,6	высокая	актуальная
17.	Перехват ПД, передаваемых по каналам связи	0	0,5	высокая	актуальная
18.	То же, внешний нарушитель	0	0,5	высокая	актуальная
19.	Несанкционированное копирование носителей информации с ПД	5	0,75	средняя	актуальная
20.	То же, внешний нарушитель	2	0,6	средняя	актуальная
21.	Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств	0	0,5	низкая	Не актуальная
22.	То же, внешний нарушитель	0	0,5	низкая	Не актуальная
23.	Непреднамеренное заражение компьютера вирусами	5	0,75	низкая	актуальная
24.	Преднамеренное заражение компьютера вирусами	10	1,0	низкая	актуальная
25.	Вмешательство в процесс функционирования ИСПДн , сетей общего пользования с целью несанкционированной модификации данных	5	0,75	высокая	актуальная
26.	То же, внешний нарушитель	2	0,6	высокая	актуальная
27.	Несанкционированное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей	10	1,0	средняя	актуальная
28.	То же, внешний нарушитель	5	0,75	средняя	актуальная
29.	Неумышленное повреждения внешних кабельных систем связи	2	0,6	низкая	актуальная
30.	Возникновение пожаров в непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.	2	0,6	высокая	актуальная
31.	Разрушение зданий, отдельных помещений	0	0,5	высокая	актуальная
32.	Возникновение стихийных очагов пожаров	2	0,6	низкая	Не актуальная
33.	Аварии в системах электропитания	5	0,75	низкая	актуальная
34.	Аварии в системах отопления и водоснабжения в непосредственной близости к помещениям, в которых обрабатываются ПД и архивам ПД	2	0,75	средняя	актуальная

Приложение к приказу по МБУ
«СШОР по легкой атлетике» № 92от
15.07.2019 г.

Муниципальное бюджетно учреждение
«Спортивная школа олимпийского резерва
по легкой атлетике»

ИНСТРУКЦИЯ

по организации учета, использования, передачи и уничтожения электронных носителей персональных данных и другой конфиденциальной информации

I. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее - носители), предназначенных для обработки персональных данных и иной конфиденциальной информации в муниципальном бюджетном учреждении «Спортивная школа олимпийского резерва» (далее – МБУ «СШОР по легкой атлетике»).

1.2. К электронным носителям информации относятся: гибкие магнитные диски, CD- и DVD-диски, USB флеш-диски, накопители на жестких магнитных дисках и др.

1.3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения персональных данных и иной конфиденциальной информации, затирание (удаление) информации возлагается на администратора информационной безопасности.

1.4. Положения данной инструкции обязательны для выполнения всеми сотрудниками МБУ «СШОР по легкой атлетике», которые в ходе выполнения своих должностных обязанностей используют носители персональных данных и иной конфиденциальной информации, а так же имеющими допуск к обработке персональных данных и иной конфиденциальной информации.

II. Учёт и хранение электронных носителей информации

2.1. Учёту подлежат все носители информации, находящиеся в распоряжении МБУ «СШОР по легкой атлетике».

2.2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации» (Приложение №1) в котором производится непосредственно регистрация и учёт носителей.

2.3. Регистрация и учет носителей информации осуществляется администратором информационной безопасности.

2.4. Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис (например: уч. № ОБ-1/К, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале, К – «Конфиденциально»).

В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из порядкового номера по журналу регистрации (например: уч. № 01/К, где 01 – порядковый номер в журнале, К – «Конфиденциально»).

2.5. Каждый носитель информации, применяемый при обработке информации на средствах вычислительной техники (далее - СВТ), должен иметь гриф конфиденциальности, соответствующий записанной на нём информации: для персональных данных и иной конфиденциальной информации - «К». Исключается хранение на одном носителе информации

разных грифов конфиденциальности, а так же хранение информации, имеющей разные цели обработки.

2.6. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.). Надпись реквизитов делается разборчиво и аккуратно. На дискеты и футляры носителей допускается наклеивать заранее заготовленную этикетку.

2.7. Каждому носителю в журнале должна соответствовать отдельная строка.

2.8. Накопители на жестких магнитных дисках (НЖМД) в серверах и системных блоках компьютеров учитываются в паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

2.9. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.10. О фактах утраты носителей необходимо незамедлительно докладывать руководителю своего структурного подразделения.

2.11. Администратор информационной безопасности не реже одного раза в год осуществляет проверку условий хранения носителей персональных данных и иной конфиденциальной информации.

III. Выдача/сдача и передача носителей

3.1. Выдача носителей сотрудникам осуществляется администратором информационной безопасности под подпись с отметкой в «Журнале выдачи/сдачи электронных носителей персональных данных и иной конфиденциальной информации» (Приложение №2). Факт сдачи носителя регистрируется аналогичным образом.

3.2. Носители, как правило, выдаются только непосредственно на время работы с данным носителем и сдаются сотрудником администратору информационной безопасности сразу по завершению таких работ.

3.3. Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случаи наличия какой-либо информации на выдаваемом носителе, администратор информационной безопасности обязан удалить (затереть) информацию согласно п. 4. настоящей инструкции.

3.4. В случае повреждения носителей, содержащих персональные данные и (или) иную конфиденциальную информацию, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и администратору информационной безопасности.

3.5. При передаче в другие организации носители информации должны, по возможности, быть упакованы в пакет/конверт, обеспечивающий сохранность (работоспособность) передаваемого носителя. При этом носители информации передаются с сопроводительным письмом, в котором указывается, какая информация содержится на данном носителе, а для подтверждения достоверности информации прилагается таблица с реквизитами файлов (допускается прикладывать скриншот окна архиватора). Данное передвижение (передача) носителей персональных данных и иной конфиденциальной информации регистрируется в «Журнале передачи носителей персональных данных и иной конфиденциальной информации» (Приложение 3), где делается отметка об отправке (куда отправлен (реквизиты адресата), исходящий номер сопроводительного письма, дата отправки, способ отправки (курьер, заказная почта и т.п.)) и отметка о получении (номер «Уведомления о вручении» или «Накладной»). В случае если передача носителей осуществляется лично сотрудником МБУ «СШОР по легкой атлетике», то у адресата, необходимо взять расписку о получении носителя (Приложение 4).

3.6. Для исключения утечки информации, находящейся на жестких дисках компьютеров, при необходимости ремонта компьютера в сервисном центре, жесткий диск с компьютера демонтируется и компьютер отправляется в ремонт без жесткого диска. При необходимости диагностирования самого жесткого диска информация должна быть предварительно скопирована на резервный носитель и затем стёрта с направляемого в ремонт винчестера с использованием специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования. Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению руководителя организации.

IV. Порядок уничтожения носителей, затирания информации на носителях

2.1.Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.

2.2.Перед уничтожением носителя вся информация с него должна быть стерта (уничтожена) путем использования специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

2.3.Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной приказом

руководителя МБУ «СШОР по легкой атлетике». В состав комиссии должен входить администратор информационной безопасности.

2.4. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт (Приложение №5). В Акте указываются учётные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Реквизиты Акта заносятся председателем данной комиссии в графу «Сведения об уничтожении» «Журнала регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации». Подписанный Акт храниться у администратора информационной безопасности.

Приложение 1
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

МБУ «СШОР по легкой атлетике»

Журнал №__
регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации

с «__»_____201_ г.

по «__»_____201_ г.

ФИО и должность ответственного за ведение журнала:_____

Журнал составлен на _____ листах

№ п/п	Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая будет содержаться на носителе	Дата регистрации электронного носителя	ФИО лица, регистри-рующего носитель	Подпись лица, регистри-рующего носитель	Сведения об уничтожении носителя (№ акта, дата)
1.	2.	3.	4.	5.	6.	7.	8.

Приложение 2
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

МБУ «СШОР по легкой атлетике»

Журнал №__
выдачи/сдачи электронных носителей персональных данных и иной конфиденциальной информации

с «__»_____201_ г.
по «__»_____201_ г.

ФИО и должность ответственного за ведение журнала:_____

Журнал составлен на _____ листах

Дата	Время	Регистрационный номер электронного носителя	Сдал		Принял	
			ФИО, должность	Подпись	ФИО, должность	подпись
1.	2.	3.	4.	5.	6.	7.

Приложение 3
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

МБУ «СШОР по легкой атлетике»

Журнал №__
передачи носителей персональных данных и иной конфиденциальной информации

с «__»_____201_ г.

по «__»_____201_ г.

ФИО и должность ответственного за ведение журнала:_____

Журнал составлен на _____ листах

Дата	Регистрационный номер электронного носителя	Характер информации, содержащейся на передаваемом носителе	Исходящий номер сопроводительного письма	Адресат (название организации, отдел, должность, ФИО и т.п.)	Способ передачи/отправки носителя (лично, курьер, заказная почта)	Отправитель (лицо, записавшее информацию на носитель)		Отметка о доставке (дата, реквизиты документа, подтверждающие доставку)
						ФИО, должность	Подпись	
1.	2.	3.	4.	5.	6.	7.	8.	9.

Приложение 4
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

№_____
заполняется отправителем

Расписка
(составлена в двух экземплярах, по одному для каждой из сторон)

«___»_____ 201_ г. г. Барнаул

Настоящим подтверждаю получение электронного носителя информации (Регистрационный номер электронного носителя_____) с сопроводительным письмом (Исходящий номер сопроводительного письма _____) от
Название организации: МБУ «СШОР по легкой атлетике»_____
Должность и ФИО представителя организации:_____
_____

Сведения о получателе:

Название организации:_____
Должность и ФИО получателя:_____
_____

«___»_____ 201_ г. _____/_____/
подпись получателя расшифровка

Приложение 5
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

МБУ «СШОР по легкой атлетике»

АКТ № ____

о затирании/уничтожении персональных данных и иной конфиденциальной информации/электронных носителей

«____»_____201_ г. г. Канск

Комиссия в составе:

Председатель:_____ (ФИО)

Члены комиссии: _____ (ФИО)

_____ (ФИО)

составила настоящий Акт о том, что в ее присутствии уничтожены следующие электронные носители персональных данных и иной конфиденциальной информации/ информация на следующих электронных носителях

Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая содержится на носителе	Причина	Способ уничтожения (физическое разрушение, форматирование, с использованием специальных программных средств (каких))
1.	2.	3.	4.	5.

Председатель комиссии: _____(ФИО)
подпись

Члены комиссии: _____(ФИО)
подпись

_____(ФИО)
подпись

Отметку в «Журнал регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации» произвел администратор информационной безопасности_____ (ФИО)_____.
подпись

Муниципальное бюджетное учреждение
Спортивная школа олимпийского резерва
по легкой атлетике

ПРИКАЗ

«15» июля 2019 г. № 94 г. Прохладный

«Об утверждении должностной инструкции ответственного за организацию обработки персональных данных и ответственного за защиту персональных данных в МБУ «СШОР по легкой атлетике»»

В соответствии с Постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:
- должностную инструкцию, ответственного за организацию обработки персональных данных в МБУ «СШОР по легкой атлетике» (Приложение № 1);
- должностную инструкцию, ответственного за защиту персональных данных в МБУ «СШОР по легкой атлетике» (Приложение № 2).

И.О. директора
МБУ «СШОР по легкой атлетике»: А.В. Цопанова

Приложение № 1
к приказу по МБУ «СШОР по легкой атлетике» № 94 от 15.07.2019 г.

Должностная инструкция
ответственного за организацию обработки персональных данных
в МБУ «СШОР по легкой атлетике»»

1. Общие положения

1.1. Настоящая должностная инструкция по обеспечению безопасности персональных данных (далее - Инструкция) определяет основные цели, функции и права специалиста ответственного за организацию обработки персональных данных в МБУ «СШОР по легкой атлетике»

1.2. Ответственный за организацию обработки персональных данных назначается приказом директора на основании Федерального Закона «О персональных данных» №152-ФЗ от 27 июля 2006 года и Постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных».

1.3. Ответственный за организацию обработки персональных данных проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспертному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.4. Непосредственное руководство работой ответственного за организацию обработки персональных данных осуществляет директор учреждения.

1.5. Ответственный за организацию обработки персональных данных назначается из числа заместителей директора учреждения, который по основной деятельности курирует вопросы кадровой работы и информатизации.

1.7. В своей работе, ответственный за организацию обработки персональных данных руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и нормативными правовыми актами администрации района по обеспечению безопасности персональных данных.

2. Основные функции, ответственного за организацию обработки персональных данных.

2.1. Проведение единой технической политики МБУ «СШОР по легкой атлетике» и координация работ по организации обработки и обеспечению безопасности персональных данных.

2.2. Планирование мероприятий по организации обеспечения безопасности персональных данных.

2.2. Организация мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2.3. Организация мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передача их лицам, не имеющим права доступа к такой информации.

2.4. Организация постоянного контроля за обеспечением уровня защищенности персональных данных.

2.8. Координация действий по подготовке объектов администрации района к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.9. Контроль за исполнением организационных распорядительных документов по организации обработки и обеспечению безопасности персональных данных в МБУ «СШОР по легкой атлетике» .

2.10. Проведение периодического контроля эффективности мер защиты персональных данных в МБУ «СШОР по легкой атлетике» . Анализ результатов контроля.

2.11. Рассмотрение предложений по устранению недостатков и предупреждению нарушений в безопасности персональных данных, осуществление контроля за устранением нарушений.

2.12. Рассмотрение и утверждение предложений по совершенствованию системы безопасности персональных данных в МБУ «СШОР по легкой атлетике».

2.13. Осуществление непосредственного контроля за соблюдением установленного законодательством порядка рассмотрения запросов субъектов персональных данных

2.14. Организация повышения квалификации сотрудников в области защиты персональных данных.

2.15. Организация повышения освещенности работников МБУ «СШОР по легкой атлетике» по вопросам обеспечения безопасности персональных данных.

2.16. Изучение отчетов о состоянии работ по обеспечению безопасности персональных данных в МБУ «СШОР по легкой атлетике».

Ответственный за организацию обработки персональных данных имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.

3.2. Осуществлять контроль за реализацией организационных и распорядительных документов по организации обработки и обеспечению

безопасности персональных данных.

3.3. Рассматривать предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность сотрудников в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Принимать решение о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать в установленном порядке необходимых специалистов из числа сотрудников МБУ «СШОР но легкой атлетике» для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

4. Ответственность, ответственного за организацию обработки персональных данных

4.1. Ответственный за организацию обработки персональных данных несет персональную ответственность за:

- правильность и объективность принимаемых решений;
- правильное и своевременное выполнение организационных и распорядительных документов, принятых администрацией МБУ «СШОР по легкой атлетике» по вопросам обработки и защиты персональных данных;
- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;

качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;

- соблюдение трудовой дисциплины, охраны труда.

С инструкцией ознакомлен:

Приложение № 2
к приказу по МБУ «СШОР по легкой атлетике» № 94 от 15.07.2019 г.

Должностная инструкция ответственного
за защиту персональных данных в МБУ «СШОР по легкой атлетике».

1. Общие положения
1.1. Настоящая должностная инструкция по обеспечению безопасности персональных данных (далее - Инструкция) определяет основные цели, функции и права специалиста по защите персональных данных (далее - Специалист) в МБУ «СШОР по легкой атлетике».
1.2. Специалист назначается приказом директора на основании Федерального Закона «О персональных данных» №152-ФЗ от 27 июля 2006 года и Постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных».
1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспертному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в Области обеспечения безопасности персональных данных.
1.4. Непосредственное руководство работой специалиста осуществляет заместитель директора, курирующий вопросы защиты информации, ответственный за организацию обработки персональных данных.
1.5. Специалист назначается из числа сотрудников МБУ «СШОР по легкой атлетике» имеющих опыт работы по основной деятельности в делопроизводстве.
1.6. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных и нормативными правовыми актами администрации района по обеспечению безопасности персональных данных.
2. Основные функции специалиста.
2.1. Уведомление органа по защите прав субъектов персональных данных об обработке персональных данных или в случае изменения сведений, указанных в Уведомлении (ч.3 ст. 22 Федерального Закона №152-ФЗ от 27.07.2006 «О персональных данных»), а также в случае прекращения обработки персональных данных.
2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию систем персональных данных.
2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных, в том числе:

- мероприятия по охране, организации доступа в помещения, где ведется обработка персональных данных;
- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятия по защите от несанкционированного доступа к персональным данным;
- мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение передачи персональных данных лицам, не имеющим права доступа к такой информации.

2.5. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.6. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.7. Участие в подготовке объектов МБУ «СШОР по легкой атлетике» к аттестации по выполнению требований обеспечения безопасности персональных данных.

2.8. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в МБУ «СШОР по легкой атлетике».

2.9. Проведение периодического контроля эффективности мер защиты персональных данных в МБУ «СШОР по легкой атлетике». Учет и анализ результатов контроля.

2.10. Организация в установленном порядке изучения причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.

2.11. Разработка предложений и участие в проводимых работах по совершенствованию системы безопасности персональных данных в МБУ «СШОР по легкой атлетике».

2.12. Ознакомление начальников отделов администрации г.о. Прохладный и специалистов с законодательством в сфере обработки и защиты персональных данных, а также с локальными нормативными правовыми актами МБУ «СШОР по легкой атлетике» по данному вопросу.

2.13. Оказание методической помощи по вопросам обеспечения безопасности персональных данных сотрудникам МБУ '«СШОР по легкой атлетике».

2.14. Подготовка отчетов о состоянии работ по обеспечению безопасности персональных данных в МБУ «СШОР по легкой атлетике».

3. Права специалиста.

Специалист имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных

данных.
3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.
3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.
3.4. Вносить предложения директору учреждения по приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.
3.6. Пользоваться необходимой помощью специалистов из числа сотрудников МБУ «СШОР по легкой атлетике» для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.
4. Ответственность специалиста.
4.1. Специалист несет персональную ответственность за:
- правильность и объективность принимаемых решений;
- правильное и своевременное выполнение распоряжений и указаний директора учреждения и его заместителя, ответственного за организацию обработки персональных данных по вопросам, входящим в возложенные на него функции;
- правильное и своевременное выполнение организационных и распорядительных документов, принятых МБУ «СШОР по легкой атлетике» по вопросам обработки и защиты персональных данных;
- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;
- согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы;
- соблюдение трудовой дисциплины, охраны труда.

С инструкцией ознакомлены:

Приложение к приказу по МБУ «СШОР
по легкой атлетике» № 92 от 15.07.2019 г.

Перечень должностей, осуществляющих обработку персональных данных МБУ «СШОР по легкой атлетике», в соответствии с законодательством Российской Федерации.

Обработка персональных данных обучающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

Право доступа к персональным данным обучающегося имеют:

- работники Министерства спорта Кабардино – Балкарской Республики;
- работники Отдела культуры, социальной политики и спорта местной администрации городского округа Прохладный КБР (при наличии соответствующих полномочий);
- директор СШОР;
- делопроизводитель СШОР;
- заместители директора;
- тренеры (только к персональным данным воспитанников своей группы);
- старший тренер;
- инспектор по охране прав детства;
- врач/медработник.

Директор СШОР осуществляет прием обучающегося в учреждение.

Директор школы может передавать персональные данные воспитанников третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья тренирующегося, в случаях, установленных федеральными законами, а так же с случае получения письменного согласия законных представителей ребенка на передачу персональных данных третьим лицам.

Делопроизводитель:

- предоставляет сведения работникам Министерства спорта Кабардино – Балкарской Республики;
- предоставляет свободный доступ родителям (законным представителям) к персональным данным воспитанникам на основании письменного заявления.

Не имеет права получать информацию о воспитаннике родитель, лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

При передаче персональных данных детей директор, делопроизводитель, заместитель директора, тренеры обязаны:

- предупредить лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены,
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.

Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных обучающегося, определяются трудовыми договорами и должностными инструкциями.

Приложение к приказу по МБУ «СШОР по легкой атлетике» № 92 от 15.07.2019 г.

Перечень
сведений ограниченного доступа МБУ «СШОР по легкой атлетике».

Персональные данные:

1. Персональные данные воспитанников

№ п/п	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
1	Устав МБУ «СШОР по легкой атлетике»	- Фамилия; - Имя; - Отчество; - дата рождения; - адрес жительства по месту регистрации; - Ф.И.О., контактная информация, степень родства законных представителей; - семейное положение; - поведенческий статус; - оказание помощи (льготы); - данные о движении воспитанника; - тренировочная деятельность (группа спортивной подготовки, результаты выступлений в соревнованиях); - промежуточная и итоговая аттестация.	Согласно номенклатуре дел, если иное не предусмотрено.

2. Персональные данные сотрудников МБУ «СШОР по легкой атлетике».

№ п/п	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
1	Трудовой Кодекс Российской Федерации	- сведения, содержащиеся в основном документе, удостоверяющем личность субъекта; - информация, содержащаяся в трудовой книжке работника; - информация,	Срок действия трудового договора + 75 лет.

		содержащаяся в страховом свидетельстве государственного пенсионного страхования; - сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу. - сведения об образовании, квалификации или наличии специальных знаний или подготовки; - сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации; - информация медицинского характера, в случаях, предусмотренных законодательством; - иные документы, содержащие сведения, необходимые для определения трудовых отношений.	